

Appl. No. 10/635,952  
Amdt. dated Jan 30, 2008  
Reply to Office action of November 30, 2007

### **REMARKS/ARGUMENTS**

Claims 1 - 4, 11 - 21 are being resubmitted. Claims 1, 11, 16 and 18 are currently amended. Claim 9 has been canceled. No new claims are being added.

Claims 1-4, 9 and 11-21 were rejected under 35 U.S.C 103(a) as being unpatentable over White et al. (U.S. Patent Application Publication 2003/0009669, hereafter White) and further in review of Ratnakar (U. S. Patent 6,522,766, hereafter Ratnakar). .

### **Summary of Examiner Interview**

Applicant hereby provides a summary of interview with the Examiner conducted on January 28, 2008.

Specifically, amended claims 1, 11 and 18 were discussed in light of White (US Patent Application 20030009669) further in view of Ratnakar (US Patent 6,522,766) regarding the unique aspects of intensity control in watermarking process, creation and use of multiple watermarked copies corresponding to "1" and "0" bits and advantageous applicability of the claimed invention to compressed audio and video.

The Examiner indicated that the claims would be considered favorably as discussed.

### **Amendments to the Claims**

Claim 1 has been amended to recite:

“a storage device containing embedment information”, the amendment being supported, for example, in paragraph **0084**;

“wherein Ce0 and Ce1 are calculated responsive to intensity of said different digital watermark,” the amendment being supported, for example, in paragraph **0052**;

“said digital content information responsive to the embedment information ; wherein the embedded information is responsive to time of digital contents distribution”, the amendment being supported, for example, at paragraphs **0018** and **0057**.

Claim 11 has been amended to recite:

“a fingerprinting information generating part generating a predetermined number of sets of Ce0 and Ce1; said partial set varied for each said acquisition requester; wherein the predetermined number is greater than one”, the amendment being supported, for example, in the abstract, in paragraph **0072**.

Claim 16 has been amended to recite:

“wherein Ce0 and Ce1 are calculated responsive to intensity of the different digital watermark”, the amendment being supported, for example, in the abstract and in paragraphs **0052**;

“wherein Ce0(n) and Ce1(n) are responsive to seed of the pseudo random number” the amendment being supported, for example, in paragraph **0084**;

“said seed being responsive to identity of the specific acquisition requester”, said amendment being supported, for example, in paragraph **0084**;

Claim 18 has been amended to recite:

“a third process for generating sequence offset information describing bit positions for raw data blocks of said digital contents; said sequence offset information used in selecting said content to output said set of contents Ce0(n) of contents Ce0 and a partial set of contents Ce1(n) of content Ce1 to generate digital watermark content Cf”, the amendment being supported, for example, in the abstract, in paragraphs **0093** and **0101**.

### **Claim objections**

Claims 16-18 were objected to for a period in the middle of the claims. Applicant respectfully submits that the currently presented claims 16-18 do not contain the deficiency.

### **White in view of Ratnakar**

Claims 1-4, 9 and 11-21, were rejected under 35 U.S.C. 103(a) as being unpatentable over White in view of Ratnakar.

Regarding Claim 1, White teaches methods of adding unique watermarks to copies of digital content. The watermark can also be used to indicate the origin and authenticity of the data or the identity of clients/users/customers of the data (paragraph 0022). The watermarks or stamps refer to any modification to one or more frames of video that result in detectable information being added to those frames (paragraph 0054). However, nowhere in the patent does White fairly teach, suggest or motivate that the watermark may include time information regarding when digital content is distributed to a requester.

Even if White is combined with Ratnakar in the sense of “a pseudo-random generator for controlling said content selector,” Ratnakar teaches a

method of watermarking (Title) using embedded information, but is silent about the specific type of embedded information beyond a general statement: "in this disclosure, the term "watermark" is used as a generic reference to essentially any type of embedded information" (column 3, lines 56-57). However, Ratnakar does not specifically motivate, teach or suggest that time of content distribution can be used as a watermarking information. Ratnakar also does not teach, suggest or motivate anywhere in the disclosure that the intensity of added watermark signal is controllable by the method of adding the watermark signal.

Therefore, the combined teachings of White and Ratnakar do not render obvious the content server distributing digital contents comprising

"a storage device containing embedment information"

"wherein Ce0 and Ce1 are calculated responsive to intensity of said different digital watermark"

"said digital content information responsive to the embedment information; wherein the embedded information is responsive to time of digital contents distribution" as claimed by the amended Claim 1.

Regarding Claim 11, White teaches methods of adding unique watermarks to copies of digital content. The watermark can also be used to indicate the origin and authenticity of the data or the identity of clients/users/customers of the data (paragraph 0022). The watermarks or stamps refer to any modification to one or more frames of video that result in detectable information being added to those frames (paragraph 0054). However, White teaches a method in which three copies of content are used: an original copy, a first copy called "a neutral copy" (paragraph 28), a second copy corresponding to sequence of 1's (paragraph 28) and a third copy corresponding to sequence of 0's (paragraph 28). Nowhere does white suggest

that multiple copies corresponding to sequence of 1's and sequence of 0's can be advantageously used to add a watermark to original content.

Even if White is combined with Ratnakar in the sense of “a pseudorandom generator for controlling said content selector,” Ratnakar does not include any discussion regarding plurality of copies of watermarked original content that can be mixed together using the pseudorandom number generator.

Therefore, the combined teachings of White and Ratnakar do not render obvious a computer for adding watermarking information, comprising

“a fingerprinting information generating part generating a predetermined number of sets of Ce0 and Ce1; said partial set varied for each said acquisition requester; wherein the predetermined number is greater than one” as claimed by the amended Claim 11.

Regarding Claim 16, the Examiner correctly comments that White does not teach using a pseudorandom generator for controlling said content generator (page 3 of Office Action). For the pseudorandom generator technique, the Examiner cites Ratnakar.

Even if White is combined with Ratnakar in the sense of “a pseudorandom generator for controlling said content selector,” to enhance the resistance of embedded information to unauthorized removal using a “seed”, the seed generation described in Ratnakar is concerned with maintaining randomness. Ratnakar described InitRNG program for generation of the pseudorandom number, using a watermark identifier M generated using MarkID program (column 9, lines 5-7). However, Ratnakar further goes on to say that “after applying the watermark, the owner stores the watermark identifier M together.” (emphasis added, column 9, lines 13-15). Thus, Ratnakar teaches a

method in which watermark is first used and then a watermark identifier is stored to associate a watermark with content. Ratnakar therefore does not fairly teach, suggest or motivate that the pseudorandom number generator is seeded by a value dependent on identity of the requester. This is different from the present method wherein watermark may be added to content by controlling the addition using a seed being responsive to identity of the specific acquisition requester.

Therefore, the combined teachings of White and Ratnakar do not render obvious the method of adding information to digital contents

“wherein Ce0 and Ce1 are calculated responsive to intensity of the different digital watermark”

“wherein Ce0(n) and Ce1(n) are responsive to seed of the pseudo random number”

“said seed being responsive to identity of the specific acquisition requester”

as claimed by the amended Claim 16.

Regarding Claim 18, while White recognizes that their method of adding watermark can be used when original content is in MPEG compressed format, (paragraph 25) their discussion on the format of storage merely points to the possibility that “[t]he content stored in content storage 106 can include video and/or audio data or other like types of data” (paragraph 25), there is not teaching, suggestion or motivation that the compressed format can be advantageously used to reduce computational complexity of adding a watermark to the content. For example, Figure 5 of White shows content storage 106 feeding content to a watermarking module 506; no sequence offset information is either generated or conveyed to the watermarking module.

Even if White is combined with Ratnakar in the sense of “a pseudo-random generator for controlling said content selector,” the combined teaching still does not teach a way to reduce computational complexity for embedding information when input digital content is in a compressed format. Ratnakar provides “a steganographic method embeds hidden information like digital watermarks” (abstract) in which “zero mean patches” are applied to images (e.g., Figures 2A, 2B, 2C and 2D). Figure 3 of Ratnakar shows that the watermarks are added to an image in *pixel domain*, which is the uncompressed representation of image input data. Nowhere in the specification does Ratnakar fairly teach, suggest or motivate suitability of the technique to apply to compressed digital data by generating sequence offset information to help with the step of adding watermark.

Therefore, the combined teachings of White and Ratnakar do not render obvious a program product for adding information to digital contents, comprising

“a third process for generating sequence offset information describing bit positions for raw data blocks of said digital contents; said sequence offset information used in selecting said content to output said set of contents Ce0(n) of contents Ce0 and a partial set of contents Ce1(n) of content Ce1 to generate digital watermark content Cf” as claimed by the amended Claim 18.

Thus, Applicant respectfully submits that White in view of Ratnakar do not make obvious the present invention as now, and that the section 103 rejection should be withdrawn.

#### CONCLUSION

Reconsideration and withdrawal of the Office Action with respect to Claims 1 – 4 and 11 – 21 is requested. Applicants submit that the claims are

Appl. No. 10/635,952  
Amdt. dated Jan 30, 2008  
Reply to Office action of November 30, 2007

now in condition for allowance or at least in better form for appeal. Applicants respectfully request that a timely Notice of Allowance be issued in this case.

In the event the examiner wishes to discuss any aspect of this response, please contact the attorney at the telephone number identified below.

The Commissioner is hereby authorized to charge payment of the following fees with this communication or credit any overpayment to Deposit Account No. 09-0441:

Any filing fees under 37 CFR 1.16 for the presentation of extra claims.

Respectfully submitted,

By: \_\_\_\_\_ / Vinay Sathe /  
Vinay Sathe  
Agent Registration No. 55,595  
Michael A. Shimokaji  
Attorney Registration No. 32, 303

SHIMOKAJI & ASSOCIATES, P.C.  
8911 Research Drive  
Irvine, CA 92618  
(949) 788-9961